(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 855 815 A2

AF

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.07.1998 Bulletin 1998/31

(51) Int. Cl.6: H04L 9/32

(21) Application number: 97120411.0

(22) Date of filing: 21.11.1997

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 22.01.1997 DE 19702049

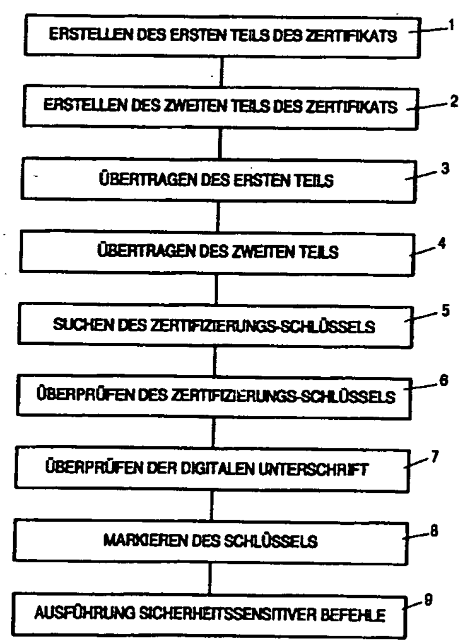
(71) Applicant:
International Business Machines Corporation
Armonk, N.Y. 10504 (US)

(72) Inventors:
- Deindl, Michael, Dipl.-Inform.
71034 Böblingen (DE)
- Hänel, Walter, Dipl.-Phys.
71088 Holzgerlingen (DE)
- Schaal, Albert, Dipl.-Ing.
72076 Tübingen (DE)

(74) Representative:
Rach, Werner, Dr.
IBM Deutschland
Informationssysteme GmbH,
Patentwesen und Urheberrecht
70548 Stuttgart (DE)

(54) Certification of cryptographic keys for chipcards

(57) The invention relates to a procedure for the certification of cryptographic keys for chipcards. In this procedure, a certification-key and a certificate are transferred to the chipcard. The first part of the certificate includes the cryptographic key and the second part of the certificate includes a digital signature of the first part of the certificate. The digital certificate is subsequently checked by means of the certification-key on the chipcard.



EP 0 855 815 A2

Description

The invention relates to the certification of cryptographic keys for chipcards.

The protection and confidential retention of data in a chipcard constitutes one of the principle advantages compared with other forms of data carriers such as magnetic strip cards or diskettes. For this reason, a form of chip hardware tailored to this purpose and various cryptographic procedures are necessary.

Amongst cryptographic procedures it is possible to distinguish between symmetrical and asymmetrical procedures. In the case of a symmetric cryptographic procedure, there exists just one key which is used both for encoding and decoding the data which can be exchanged with the chipcard. This key must be kept secret as anyone who knows this key can also read information consisting of the encoded data. This gives rise to the problem of how this key can be exchanged between the communicating partners. It is not possible to pass on the key over public networks because subsequently the key would no longer be of a secret nature.

This problem is partially resolved by the assistance of asymmetric cryptographic procedures. In this situation there is a key V for encoding and a key E for decoding. The particular point here is that only one of the two keys has to be kept secret. The key V is known to the general public while the key E is secret. If the sender wishes to send a secret message to a receiving party, he uses the publicly-known key V to encode the information. When the receiving party receives the encoded information, he can decode it with the aid of secret Key E. Naturally, the reverse situation is also conceivable where the Key V is secret and the Key E is known to the general public.

The asymmetric cryptographic procedures solve the problem of exchanging the keys. However, a new problem then arises. The authenticity of the publicly-known key must be checked. This takes place by the publicly-known key being certified by a trustworthy authority. To this end, a certificate is produced which demonstrates the following component parts:

A publicly-known key

- The name of the owner of the publicly-known key

The applications / application areas for which this publicly-known key may be used, and
A digital signature of the trustworthy authority.

From an information-technology point of view, the digital signature amounts to a kind of cryptographic check-sum of the other components of the certificate similar to a MAC (Message Authentication Code) through a prescribed data string. The trustworthy authority uses the digital signature to confirm that the elements of data (components) in the certificate belong to one another.

There is a standard for the construction and format of a certificate, namely X.509. This Standard arose in association with large data banks and therefore presupposes access to computers with high performance capacities. The evaluation of an X.509 Certificate with the aid of the processor of a chipcard is not possible.

Therefore, in the use of asymmetric cryptographic procedures with chipcards, the chipcard only serves in the first place for the retention of a key. Against this, authorisation for the use of this key with the asymmetric cryptographic procedure is achieved outside the chipcard by using a computer with a larger computing capacity.

It is the task of the present invention to create an improved opportunity for the certification of cryptographic keys for chipcards.

This task is discharged by the technical principles revealed in the independent Claims 1 and 17.

The essential advantage which is attained by the invention as compared with the current state of the art is that a certifying cryptographic key can be incorporated in the chipcard. In this way, the functionality of asymmetric cryptographic procedures is completely integrated in chipcards. A new level of security is generated and the area of possible applications for chipcards is extended. This is achieved by means of a certificate which is simple in its structure, is tailor-made for chipcards and which can be used in a certification procedure which is capable of being carried out on chipcards.

An extension of the invention provides that the checking of the digital signature on the chipcard embraces the following steps: the conversion of the digital signature on the chipcard by means of the certification-key; the generation of an electronic fingerprint for the first part of the certificate; and the comparison of the converted digital signature with the electronic fingerprint of the first part of the certificate. In this manner, non-encoded data is advantageously compared, encrypted and decrypted.

The checking of the digital signature on the chipcard can suitably include the following steps: the production of an electronic fingerprint in the first part of the certificate; conversion of the electronic fingerprint by means of the certification-key and a set of equations; and comparison of the converted electronic fingerprint with a reference value which is transferred to the chipcard with the certificate.

In this way, the encoding- and decoding operations are eliminated since uncoded data is used in the equations.

By means of an appropriate application of the invention, the cryptographic key is marked as a certificated key in the case when in the course of checking the digital signature, the latter is verified as the digital signature of the first part of the certificate. It can be made certain in this way that only those keys which have been correctly transferred to the chipcards and correctly stored in the chipcards can be used as certificated keys. Because of the marking, when a cryptographic key is being used, the status of the cryptographic key can be determined with very little effort.

A check can advantageously be made to establish whether or not the certification-key for certifying the cryptographic key can be used. This ensures that to certify cryptographic keys, exclusively only those certification keys can be used, which themselves have been previously certified for this purpose by a ' trustworthy authority'.

An advantageous form of the invention provides that the certificated key is used for the execution of security-sensitive instructions, whereby the security standard of a chipcard is improved.

The certificated key can usefully be used as a further certification-key for the certification of a further cryptographic key. In this way, any kind of certification chain can be produced.

An advantageous extension of the invention provides that the cryptographic key can be used for the execution of non-security-sensitive instructions after the certificate has been transferred to the chipcard. This makes it possible to integrate the cryptographic key into feasible applications of the chipcard even before the conclusion of the certification.

A hash-value can advantageously be calculated by means of the hash-algorithm during the production of either the digital signature of the first part of the certificate or the electronic fingerprint of the first part of the certificate. This compresses the data to be processed during the certification activity and subsequently this data can be processed with less expenditure of time and effort in the course of further certification procedures.

By means of an advantageous form of the invention, it can be provided that the first and second parts of the certificate are transferred to the chipcard independently of one another, thus rendering illegal access to the certificate more difficult. Furthermore, with the aid of the separated transfer activities, the processing of the certificate on the chipcard can be given a more efficient form. In particular, one part of the certificate can be processed off-line while the other part is processed on-line.

A useful extension of the invention can be formed in such a way that the first part of the certificate includes administrative data. In particular, this makes it possible for the limiting conditions for the use and application of the cryptographic key to be determined.

In a useful form of the invention, the cryptographic key is assigned by the administrative data to one or more applications of the chipcard whereby those applications for which the key may be used can be ascertained in an unambiguous manner. Any misuse of the cryptographic key for other applications is thereby prevented.

An advantageous form of the invention provides that during personalisation of the chipcard, the certification -key is transferred to the latter with the result that the certification key together with other security-relevant data is loaded onto the chipcard.

The marking of the cryptographic key as a certificated key can advantageously be effected by the placement of a bit in a status-byte of the cryptographic key. This illustrates a possibility for marking the certified key which can easily be evaluated by the processor of the chipcard.

By means of an advantageous form of the invention, it can be provided that the marking of the cryptographic key as a certified key can be carried out by entering the cryptographic key in a table on the chipcard. In this way, all certificated keys can be stored in the chipcard in a manner which can be inspected.

The marking of the cryptographic key as a certified key can be usefully carried out by storing the cryptographic key in a particular memory storage area of the chipcard. In order to use this cryptographic key at a later date, this calls for an exclusive reference to the particular memory storage area.

The dependent subordinate claims of Claim 17 demonstrate the advantages of the corresponding procedure claims which are dependent upon them.

An advantageous extension of the invention provides that the administrative data includes an indication of a path of a memory storage area on the chipcard, whereby the cryptographic key is exclusively storable in this area of memory storage. In this way, a definite area of memory storage on the chipcard which adequately satisfies security standards can be assigned to the cryptographic key.

In what follows, an example of an application of the invention is explained in greater detail by reference to a drawing:

In this context, Fig. 1 shows a sequence diagram of a certification procedure.

Certificates, which are used on a chipcard in accordance with the invention-based certification of cryptographic keys exhibit two parts: A first part which includes the actual data inclusive of the cryptographic key and a second part, the digital signature of the data from the first part.

As shown in Fig. 1, the first part of the certificate is produced in the course of a certification procedure. The first part refers to components as shown in Table I.

Table I

Components	Byte	Description	
1	0	Bit 7 :	0 = secret key
			1 = public key
		Bit 6 -0: key identification	
2	1	Algorithm-identification	
3	2	Hash-algorithm-identification	
4	3	Padding-algorithm-identification	
5	4	Use Byte 0	
6	5	Use Byte 1	
7	7	Nominal key length in bits	
8	9	Length of a data block	
9	10	Length of a signature	
10	11	Length of the user information	
11	12	Items of user information	
12	13	Length of the key data	
13	15	Key data	

By means of Component 1 of the certificate it is shown whether the certificating cryptographic key is a public or a secret key. Furthermore, Component 1 of the first part of the certificate also displays a key identification. It indicates permitted applications of the cryptographic key held in the certificate. If, following the completion of a successful certification, the cryptographic key is used in carrying out a specific application, this key identification is challenged and inspected to check that the certificated key can be used for the specific application. Depending upon the outcome of this interrogation, either the cryptographic key can be used or an error announcement is given.

With the aid of the following Components 2, 3 and 4, algorithm-identifications are given. Component 2 indicates the asymmetric cryptographic procedures for which the key to be certified is suitable. When the certificated key is employed, for example, a hash-algorithm and/or a padding algorithm can be used. This is determined with the aid of Components 3 and 4. The purpose of the hash-algorithm is to compress the data. The compression is carried out before the actual encoding/decoding takes place. By using the padding-algorithm, data can be extended to fill up any necessary block length.

With the aid of Components 5 and 6, application areas of the cryptographic key can be established. For example, with the aid of Component 5, it can be ascertained that the cryptographic key may only be used exclusively for the production of electronic signatures. Component 7 advises the length in bits of the cryptographic key, which is to be certificated with the aid of the certificate. Components 8, 9 and 10 make it possible to transfer block-length data to a user of the cryptographic key.

Component 11 supplies text information about the cryptographic key. In particular, this can relate to application-or security advice for the user. Component 12 indicates the actual length of the cryptographic key to be certified. Data relating to the key are to be found in Component 13.

After the first part of the certificate has been produced in accordance with Table I, the operation continues in accordance with Fig. 1 with the preparation of the second part of the certificate. To do this, an electronic signature of the first part of the certificate is produced. An electronic signature serves, principally, to establish the authenticity of electronically-transferred information or of electronic documents. In the case of certification procedures in accordance with the invention, checking of the digital signature makes it possible to determine whether the certificate was transferred to the chipcard without being modified.

The sequence followed during the production of a digital signature may be illustrated as given below. A hash-algorithm is used to develop a hash-value from the first part of the certificate. The purpose of the hash-algorithm is to compress the data forming the first part of the certificate. The hash-value is also described as the finger-print of the relevant data. After this, the hash-value is decoded with a crypto-algorithm, for example, the RSA. To decode this, one uses the secret key of a pair of keys which is entered as part of the appropriate certification procedure. The public key of this pair

of keys, i.e. of the certification keys, is found on the chip card. The reason for a decoding operation during the preparation of a digital signature is based upon the convention that with the RSA-algorithm, the secret key is always used for decoding and the public key is always used for encoding. The result of the decoding operation is the actual signature which is the content of the second part of the certificate.

The procedure followed in accordance with the invention can also be carried out in an advantageous manner with any other chosen procedure on the basis of a pair of keys containing a secret and a public key. Pairs of keys can also be used, during the application of which no explicit decoding/encoding is carried out. In particular, procedures in which the resolving of a mathematical equation for the parameters hash-value, secret key and public key is the pre-requisite for carrying out the asymmetrical procedure can be used.

After the first and second parts of the certificate have been generated, both can be transferred to the chipcard. The two parts of the certificate can be transferred to the chipcard together or independently of one another. Separated transfer procedures have the advantage that the amounts of data to be transferred to the relevant processes are smaller and, consequently, these quantities of data are easier to process.

After the first part of the certificate has been stored in the chipcard, the cryptographic key held there can first be used for the non-critical, non-security-sensitive operations on the chipcard. These non-critical operations include, in particular, the simple checking of a digital signature where in this case, the result of the checking activity will only be passed to an item of equipment which is in communication with the chipcard, but where, however, no change of status or any other changes take place in the card.

As shown in Fig. 1, during the next step, a search is made for a certification key in the card. This certification key is the public key of the stated pair of keys and must be authorised to release the certification and must, itself, already have been certificated. This means that it must be completely integrated in the chipcard. Preferably, the certification key should be installed and certified by the issuer of the card in the context of the personalisation of the chipcard. However, certification keys can also be introduced into the chipcard at a later date after the personalisation activity has been completed. The pre-requisite is that the certification key is applied to the chipcard in circumstances which satisfy the appropriate security standards.

After the check has been made to ensure that the certification-key for the certification of the certificate transferred to the chipcard may be used, the second part of the certificate which constitutes the digital signature is converted with the aid of the certification key. For this operation, the digital signature is encoded in accordance with the convention of the RSA-algorithm. The result of the calculation is a hash-value.

Furthermore, the fingerprint of the first part of the certificate, which is similarly a hash-value, is calculated on the chipcard. The fingerprint is then compared with the result of the encoding operation described in the foregoing section. If both agree with one another the cryptographic-key contained in the certificate is marked as a certificated key.

Other cryptographic procedures may be used to test that the transfer of the certificate to the chipcard has been properly carried out and then to certify the transferred key. For example, the known DSA-procedure(DSA-digital signature algorithm) can be named. In this case, a value r is calculated for the first part of the certificate by means of the secret key of the pair of keys and other mathematical parameters using generally known equations.

After the certificate has been transferred, the value r is used on the chipboard with the aid of further known equations in combination with the transferred certificate and the public key of the of the pair of keys to calculate a value v. If r and v agree with one another, the cryptographic key is marked as a certificated key. Use of the hash-algorithm is also made when using the DSA-procedure. Still other asymmetric procedures can be used for the certification activity if they guarantee the necessary standard of security.

The marking of a cryptographic key as ' certificated' can be achieved, in particular, by means of placing a bit in a status-byte associated with the cryptographic key. However, other procedures for marking are conceivable. These include the storing of the cryptographic key in a specific memory area of the chipcard or the establishment of a list containing all the cryptographic keys which have been marked as certificated.

The decision as to which form of marking will be chosen depends, in particular, upon the architecture of the relevant chipcard and its applications.

After the marking activity for the cryptographic key has been completed, the certificated key can be used for the security-sensitive operations. The marking is interrogated on every occasion that a cryptographic key is accessed. Once the certification has been concluded, the certificated key is stored in the chipcard together with the accompanying data (see the components of the first part of the certificate). The accompanying data can be interrogated each time the key is accessed but also interrogated to provide information about the key.

If a certificated key is required in order to carry out a security-sensitive operation on the chipcard, the required cryptographic key is only used for that operation if its marking shows that a certificated key is involved. If the questioning of the marking produces a negative result, i.e. it is not a case of a certificated key, an error annoncement is given. In particular, external authorisation forms part of the security-sensitive operations. This involves checking of the identity and authenticity of a communication partner of the chipcard. The chipcard and its communication partner (e.g. a terminal) mutually establish whether or not the communication partner is a genuine terminal or a genuine chipcard.

An essential advantage of the certificate in accordance with Table I is that with the aid of informal data held in the certificate, the cryptographic key can be assigned to a specific application. This is of great importance, particularly in the area of the chipcard because here cryptographic keys must be assigned to individual applications rather than to individual persons. These applications can, for example, include a group of similar automatic cash point machines.

The digital determination of the application areas in the certificate (preferably by means of components 1, 5 and 6) provides the opportunity of excluding the possibility of misusing the cryptographic key for other applications.

If a certificated key is used in the context of carrying out a specific application, at the commencement of the access to this certificated key there will be a challenge as to whether the certificated key is authorised for the specific application. This can be done by means of the certificated information in the first part of the certificate. This information was stored in the chipcard together with the cryptographic key after certification had been completed.

If data is included in the applications of the chipcard, this is present in the form of data files. These data files possess attributes which are determined, for example, by the party issuing the chipcard. Preferably, these attributes include a reference to the key identification of the certified key which must be used for a specific operation with the relevant data files. This key identification in the attribute must then agree with the key identification of the certificated key (Component 2 of the certificate). If this should not be the case, the operation is not carried out. In this way, any improper use of a certified key is prevented.

Claims

1. Procedure for the certification of a cryptographic key for a chipcard, with the following procedural steps:

    a) Transfer of a certification-key to the chipcard,

    b) Transfer of a certificate to the chipcard, whereby a first part of the certificate includes the cryptographic key and a second part of the certificate includes a digital signature of the first part of the certificate, and

    c) Testing the digital signature by means of the certification-key on the chipcard.

2. Procedure in accordance with Claim I characterised in that the testing of the digital signature on the chipcard includes the following steps:

    c1) Conversion of the digital signature by means of the certification-key,

    c2) Production of an electronic fingerprint of the first part of the certificate, and

    c3) Comparison of the converted digital signature with the electronic fingerprint of the first part of the certificate.

3. Procedure in accordance with Claim I characterised in that the testing of the digital signature on the chipcard includes the following steps:

    c1) Production of an electronic fingerprint of the first part of the certificate,

    c2) Conversion of the electronic fingerprint by means of the certification-key and a set of equations, and

    c3) Comparison of the converted electronic fingerprint with a reference value which is transferred onto the chipcard with the certificate.

4. Procedure in accordance with Claim I distinguished by a further procedural step:

    Marking of the cryptographic key as a certified key in the event that when the digital signature is checked, this is verified as being the same as the digital signature of the first part of the certificate.

5. Procedure in accordance with Claim 1 distinguished by a further procedural step:

    Checking whether or not the certification-key can be used to certify the cryptographic key.

6. Procedure in accordance with Claim 4 distinguished by a further procedural step:

   Using the certificated key for carrying out security-sensitive instructions.

7. Procedure in accordance with Claim 1 characterised in that the certificated key is used as a further certification-key for the certification of a further cryptographic key.

8. Procedure in accordance with Claim 1 characterised in that

   the cryptographic key can be used for the execution of a non-security-sensitive instruction after the certificate has been transferred to the chipcard.

9. Procedure in accordance with Claims 2 or 3 characterised in that

   on each occasion when producing the digital signature of the first part of the certificate and when producing the electronic fingerprint of the first part of the certificate a hash-value is calculated by means of the hash-algorithm.

10. Procedure in accordance with Claim 1 characterised in that

    the first part and second part of the certificate are transferred to the chipcard independently of one another.

11. Procedure in accordance with Claim 1 characterised in that

    the first part of the certificate includes administrative data.

12. Procedure in accordance with Claim 11 characterised in that

    the cryptographic key is assigned to one or several applications of the chipcard by means of the administrative data.

13. Procedure in accordance with Claim 1, characterised in that

    the certification-key is transferred to the chipcard during personalisation of the chipcard.

14. Procedure in accordance with Claim 4 characterised in that

    the marking of the cryptographic key as a certificated key is carried out by means of setting a bit in a status-byte of the cryptographic key.

15. Procedure in accordance with Claim 4 characterised in that

    the marking of the cryptographic key as a certificated key is carried out by means of an entry of the cryptographic key in a table in the chipcard.

16. Procedure in accordance with Claim 4 characterized in that

    the marking of the cryptographic key as a certificated key is carried out by storing the cryptographic key in a given memory area of the chipcard.

17. Certificate for certification of a cryptographic key for a chipcard,
    characterised by

    a first part and a second part, whereby the two parts are separated from one another

    and whereby the first part includes the cryptographic key and the second part includes a digital signature of the first part.

18. Certificate in accordance with Claim 17 characterised in that

the certificate is capable of being transferred to the chipcard and can be evaluated by a processor on the chipcard.

19. Certificate in accordance with Claim 17
characterised in that

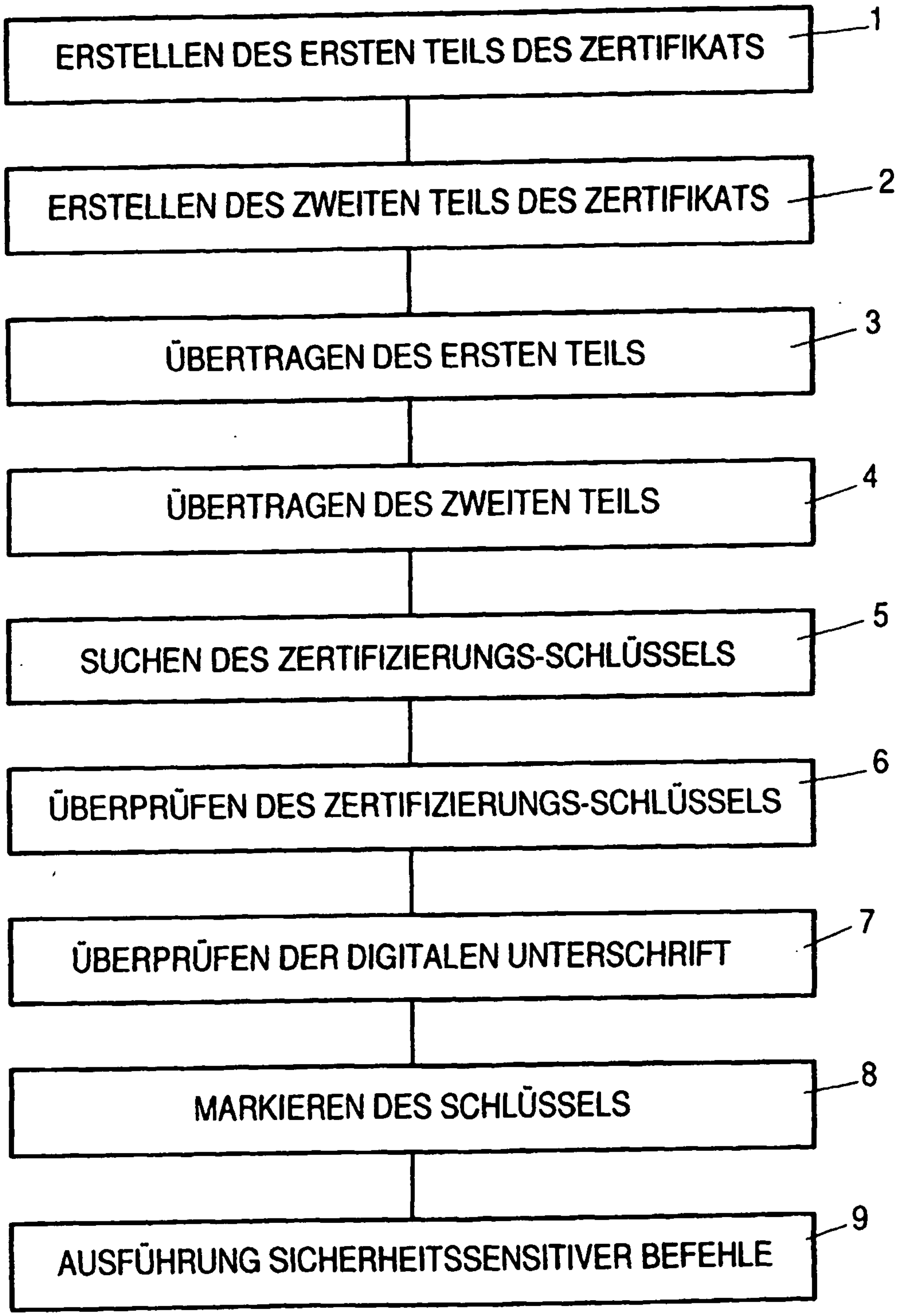
the first part of the certificate includes administrative data.

20. Certificate in accordance with Claim 19 characterised in that

the cryptographic key is capable of being assigned to one or several applications by the administrative data, and

by means of the administrative data, it is possible to prevent any misuse of the cryptographic key for other applications which differ from the one or several applications.

21. Certificate in accordance with Claim 19, characterised in that the administrative data includes the indication of a path of a memory storage area on the chipcard, whereby the cryptographic key can be stored exclusively in this memory storage area.


ERSTELLEN DES ERSTEN TEILS DES ZERTIFIKATS
1
ERSTELLEN DES ZWEITEN TEILS DES ZERTIFIKATS
2
ÜBERTRAGEN DES ERSTEN TEILS
3
ÜBERTRAGEN DES ZWEITEN TEILS
4
SUCHEN DES ZERTIFIZIERUNGS-SCHLÜSSELS
5
ÜBERPRÜFEN DES ZERTIFIZIERUNGS-SCHLÜSSELS
6
ÜBERPRÜFEN DER DIGITALEN UNTERSCHRIFT
7
MARKIEREN DES SCHLÜSSELS
8
AUSFÜHRUNG SICHERHEITSSENSITIVER BEFEHLE
9